U.S. Department of Justice

THE USA PATRIOT ACT: MYTH VS. REALITY

SEPTEMBER 2003

THE USA PATRIOT ACT:
MYTH VERSUS REALITY

In October of 2001, Congress passed (98-1 in the Senate; 357-66 in the House) and the President signed into law the USA PATRIOT Act, a vital tool in the continuing effort to prevent future acts of terrorism. Sixteen of the provisions in this Act - those considered to be "new" authorities - are scheduled to sunset December 31, 2005.

There has been much interest in this law, and unfortunately, much disinformation about the scope of its application and the breadth of its authorities. This booklet was prepared in an effort to provide information regarding key provisions of the USA PATRIOT Act - including information about the civil liberties protections included in its text, information about the involvement and supervision of federal courts regarding the use of many of its authorities, and information about how this law has contributed to America's successes in the war on terrorism.

This law has already been the subject of rigorous, and appropriate, Congressional oversight. This oversight is important and helpful, and it is a necessary part of our democratic process of government. Additional information about Congressional oversight of the USA PATRIOT Act, including over 100 pages of questions and answers about the USA PATRIOT Act submitted to the House Judiciary Committee, can be found at www.lifeandliberty.gov.

The USA PATRIOT Act:

MYTH VS. REALITY

Table of Contents

WINNING THE WAR ON TERRORISM

General:

- For decades, terrorists have waged war against U.S. interests. Now America is waging war against terrorists.

- As the President has said, "Free people will set the course of history." We have expanded freedom over the past two years while protecting civil liberties and protecting people here and around the world from further terrorist attacks.

- The United States of America is winning the war on terrorism with unrelenting focus and unprecedented cooperation. Prevention of terrorist attacks is our first priority and with the President taking the lead, information sharing and cooperation has vastly increased today. We are better able to "connect the dots."

- The Department of Justice has acted thoughtfully, carefully and within the framework of American freedom -- the Constitution of the United States. Survival and success in this long war on terrorism demands that the Department continuously adapt and improve its capabilities, as terrorists do, to protect Americans from a fanatical, ruthless enemy.

- The Department will continue to seek the assistance of Congress as it builds a culture of prevention and ensures the resources of our government are dedicated to defending Americans.

How we are winning the war on terrorism:

- **First, we are disrupting, arresting and detaining potential terrorist threats:**

  - ✓ The FBI and our partners, both here and abroad, have identified, disrupted and neutralized over 100 terrorist threats and cells;
  - ✓ Worldwide, more than half of al Qaeda's senior leadership has been captured or killed;
  - ✓ Worldwide, more than 3,000 operatives have been incapacitated;
  - ✓ 4 alleged terrorist cells in Buffalo, Detroit, Seattle and Portland have been broken up;
  - ✓ 255 criminal charges have been brought to date;
  - ✓ 132 individuals convicted or pled guilty, including shoe-bomber Richard Reid, "American Taliban" John Walker Lindh, six members of the Buffalo cell who have pled guilty and are cooperating; two members of the Detroit cell, as well as Iyman Faris; and
  - ✓ Over 515 individuals linked to the September 11 investigation have been deported.

- **Second, we are gathering and cultivating detailed intelligence on terrorism in the U.S.:**

- ✓ Hundreds of suspected terrorists have been identified and tracked throughout the United States;
- ✓ Our human sources of intelligence have doubled;
- ✓ Our counter-terrorism investigations have doubled in one year;
- ✓ 18,000 subpoenas and search warrants have been issued; and
- ✓ In 2002, over 1,000 applications were made to the FISA court targeting terrorists, spies and foreign powers who threaten our security, including 170 emergency FISAs.

- **Third, we are gathering information by leveraging criminal charges and long prison sentences.** When individuals realize that they face a long prison term, they often try to cut their prison time by pleading guilty and cooperating with the government.

  - ✓ Since September 11, we have obtained criminal plea agreements from more than 15 individuals, who must, and will continue to, cooperate with the government in its terrorist investigations.
  - ✓ These individuals have provided critical intelligence about al Qaeda and other terrorist groups, safehouses, training camps, recruitment, and tactics in the U.S., and the operations of those terrorists who mean to do American citizens harm.
  - ✓ One individual has given us intelligence on weapons stored here in the United States.
  - ✓ Another cooperator has identified locations in the U.S. being scouted or cased for potential attacks by al Qaeda.

- **Fourth, we are dismantling the terrorist financial network:**

  - ✓ 36 designated terrorist organizations;
  - ✓ $133 million in assets frozen around the world;
  - ✓ 70 investigations into terrorist financing, with 23 convictions or guilty pleas to date.
  - ✓ The FBI set up a Terrorist Financing Operations Section (TFOS). TFOS identifies, investigates, prosecutes, disrupts and dismantles terrorist related financial and fundraising activities.

- **Fifth, we are using new legal tools to detect, disrupt, and prevent potential terrorist plots.** Congress has provided better crime-fighting tools to make sure we are doing all we can, legally and within the bounds of the Constitution, to detect, disrupt and prevent acts of terror.

  - ✓ <u>The PATRIOT Act</u>: Senate vote 98-1; House vote 357-66

    1) Passed with overwhelming bipartisan majorities, the PATRIOT Act allows investigators to use the same tools that were already available in the war on crime and drugs to prosecute the war on terrorism. These tools have been used for decades and have been reviewed and approved by the courts.

    2) Removed the legal barriers that prevented the law enforcement, intelligence, and defense communities from sharing information. Our prevention efforts cannot be constrained by boxes on an organizational chart.

3) Brought the law up to date with current technology, so we no longer have to fight a digital-age battle with antique weapons - legal authorities leftover from the era of rotary telephones.

4) Increased the penalties for those who commit terrorist crimes. Americans are threatened as much by the terrorist who pays for a bomb as by the one who pushes the button. That's why the PATRIOT Act imposed tough new penalties on those who commit and support terrorist operations, both at home and abroad.

- **Sixth, we are building our long-term counter-terrorism capacity:**

  - ✓ A near three-fold increase in counter-terrorism funds;
  - ✓ Over 1,000 new and redirected FBI agents dedicated to counter-terrorism and counter-intelligence;
  - ✓ 250 new Assistant U.S. Attorneys;
  - ✓ 66 Joint Terrorism Task Forces;
  - ✓ 337% increase in Joint Terrorism Task Force staffing; and
  - ✓ FBI Flying Squads developed for rapid deployment to hot spots worldwide.

- **Time and again, the Department has successfully defended legal challenges including:**

  - ✓ Enemy combatant detention authority – SUSTAINED
  - ✓ Guantanamo Bay detention authority – SUSTAINED
  - ✓ FISA information sharing authority – SUSTAINED
  - ✓ Withholding names of sensitive immigration detainees – SUSTAINED
  - ✓ President's authority to freeze assets of purported charities that fund terrorists – SUSTAINED

- **No provision of the USA PATRIOT Act has been held unconstitutional by any court.**

Section 201. Authority to intercept wire, oral, and electronic communications relating to terrorism.

- Summary: Allows law enforcement to use the existing electronic-surveillance authorities to investigate certain crimes that terrorists are likely to commit.

- Myth: "Because the government already had substantial authority under FISA to obtain a wiretap of a suspected terrorist, the real effect of this amendment is to permit wiretapping of a United States person suspected of domestic terrorism." [Electronic Privacy Information Center (EPIC), Mar. 19, 2003]

- Reality:

  - ✓ Before the PATRIOT Act, law enforcement had the authority to conduct electronic surveillance – by petitioning a court for a wiretap order – when investigating many **ordinary, non-terrorism crimes**. Agents also could use wiretaps to investigate some, but not all, of the crimes that terrorists often commit.

    - ➢ The non-terrorism offenses for which wiretaps were available included: drug crimes, mail fraud, and passport fraud.

  - ✓ Section 201 enabled investigators to gather information when looking into the **full range of terrorism-related crimes**, including: chemical-weapons offenses, the use of weapons of mass destruction, killing Americans abroad, and terrorism financing.

  - ✓ Section 201 **preserved all of the pre-existing standards** in the wiretap statute. For example, law enforcement still must: (1) apply for and receive a **court order**; (2) establish **probable cause** that criminal activity is afoot; and (3) first have tried to use "**normal investigative procedures**."

  - ✓ Section 201 has proven to be extremely useful to law enforcement officials, as several recent wiretap orders have been based on this expanded list of terrorism offenses.

  - ✓ This provision will sunset on December 31, 2005.

Section 203. Authority to share criminal investigative information.

- Summary: Permits sharing of grand jury and wiretap information regarding foreign intelligence with federal law-enforcement, intelligence, protective, immigration, national-defense and national-security personnel.

- Myth: "While some sharing of information may be appropriate in some limited circumstances, it should only be done with strict safeguards. . . . The bill lacks all of these safeguards. As a result it may lead to the very abuses that the Church Committee exposed decades ago." [American Civil Liberties Union (ACLU), Oct. 23, 2001]

- Reality:

  - ✓ **Before USA PATRIOT**, federal law sharply limited the ability of federal law-enforcement to share terrorism-related information with national-defense officials and members of the intelligence community in order to protect the American People from terrorism. As the **recent 9/11 Congressional Joint Inquiry Report confirms, prior to September 11th our ability to connect the dots was inhibited** by the inability to coordinate throughout our own government.

    - ➢ For example, suppose that a federal prosecutor learned during grand jury testimony that terrorists were planning to detonate a nuclear bomb in Manhattan in the next 30 minutes. **Federal Rule of Criminal Procedure 6(e) would have prevented him from immediately notifying national-security officials.**

  - ✓ Section 203 facilitated a **coordinated, integrated antiterrorism campaign** by allowing the sharing of information acquired by wiretaps or through grand jury proceedings. Thanks to section 203, the right hand now knows what the left hand is doing.

  - ✓ Section 203 contains a number of **privacy safeguards**. An individual who receives any information under this section can use it only "**in the conduct of that person's official duties.**" And any time grand jury information is shared, the government is required to **notify the supervising court**.

  - ✓ On September 23, 2002, the Attorney General issued **privacy guidelines** governing the sharing of information that identifies a United States person. These rules require that all such information be labeled before disclosure, and handled according to specific protocols designed to ensure its appropriate use.

  - ✓ The Department has made disclosures of vital information to the intelligence community and other federal officials under section 203 on dozens of occasions.

  - ✓ The authority to share wiretap information will sunset on December 31, 2005. The authority to share grand jury information **will not** sunset.

Section 206. Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

- Summary: Allows FISA court to authorize "roving surveillance" when it finds that the target's actions may thwart the identification of a communications company or other person whose assistance may be needed to carry out the surveillance.

- Myth: "These wiretaps pose a greater challenge to privacy because they are authorized secretly without a showing of probable cause of crime…This Section represents a broad expansion of power without building in a necessary privacy protection." [ACLU, Oct. 23, 2001]

- Reality:

  - ✓ **For years, law enforcement has been able to use "roving wiretaps"** – in which a wiretap authorization attaches to a particular suspect, rather than a particular communications device – **to investigate ordinary crimes**, including **drug offenses** and **racketeering**. The authority to use roving wiretaps in drug cases has existed since 1986.

  - ✓ Section 206 authorized the **same techniques in national-security investigations**. This provision has enhanced the government's authority to monitor sophisticated international terrorists and intelligence officers, who are trained to thwart surveillance, such as by rapidly changing cell phones, just before important meetings or communications.

  - ✓ A wiretap under section 206 can be ordered only after the FISA court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance.

  - ✓ A number of federal courts – including the Second, Fifth, and Ninth Circuits – have squarely ruled that roving wiretaps are perfectly consistent with the Fourth Amendment.

  - ✓ Whether the Department has used section 206 is classified. Details about its use were provided to the House Permanent Select Committee on Intelligence on May 29, 2003, in response to a request by the House Committee on the Judiciary.

  - ✓ This provision will sunset on December 31, 2005.

Section 209. Seizure of voice-mail messages pursuant to warrants.

- Summary: Allows law enforcement to obtain voice mail stored with a third party provider by using a search warrant, rather than a wiretap order.

- Facts:

  - ✓ Under previous law, law enforcement could use a search warrant to obtain voice messages stored on an answering machine inside a terrorist's home. But agents had to go through the burdensome process of obtaining a wiretap order if the same messages were stored with a third party provider.

  - ✓ Section 209 allowed investigators, upon a showing of **probable cause**, to use **court-issued search warrants to obtain voicemails** held by a third-party provider. Simply put, the law now treats these voicemail messages the same as voicemails on a home answering machine.

  - ✓ Section 209 **preserved all of the pre-existing standards** for the availability of search warrants. For example, law enforcement still must: (1) apply for and receive a **court order**; and (2) establish **probable cause** that criminal activity is afoot.

  - ✓ Since passage of the Act, such warrants have been used in a variety of criminal cases to obtain key evidence, including voicemail messages left for foreign and domestic terrorists.

  - ✓ Under previous law, the wiretap statute governed access to stored wire communications such as voicemail, because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications.

  - ✓ This provision will sunset December 31, 2005.

Section 210. Scope of subpoenas for records of electronic communications.

- Summary: Broadens the types of records that grand juries can subpoena from electronic communications providers to include the means and source of payment, such as bank accounts and credit card numbers.

- Facts:

  - ✓ **Before USA PATRIOT**, federal law allowed grand juries to subpoena a **limited class of information from electronic-communications providers**. Grand juries could not subpoena certain information – such as credit card and bank account numbers – that is indispensable in tracking down a suspect's true identity.

  - ✓ **Section 210 updated the law** by allowing grand juries to subpoena **the full range of information** necessary to determine suspects' identities. Now, grand juries can issue subpoenas for the means of payment that customers use to pay for their accounts. That includes "any credit card or bank account number."

    - ➢ This information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information.

  - ✓ Prosecutors in the field report that this new authority has allowed for quick tracing of suspects in numerous important cases, including several terrorism investigations and a case in which computer **hackers attacked over fifty government and military computers**.

  - ✓ As is true of all subpoenas, recipients of a section 210 subpoena can go to court and **ask the judge to quash it**. And, if the recipient refuses to comply with a section 210 subpoena, the government must **ask a judge to enforce it**; agents **cannot** enforce it unilaterally.

  - ✓ Before section 210, grand jury subpoenas of electronic-communications providers generally were limited to obtaining customers' names, addresses, and length of service.

Section 211. Clarification of scope.

- Summary: Clarifies that the statutes governing telephone and Internet communications – not the burdensome provisions of the Cable Act – apply to cable companies that provide Internet or telephone service.

- Facts:

  - ✓ Before the USA PATRIOT Act, some cable companies, citing restrictions in the federal Cable Act, **ignored lawful court orders** requiring them to turn over records about their customers' Internet or telephone use – even though any other Internet or telephone provider would have had to comply.

  - ✓ Section 211 clarified that when a cable company provides telephone or Internet service, **it must comply with the same disclosure laws** that apply to any other telephone company or Internet service provider.

    - ➢ Terrorists no longer can exempt themselves from lawful investigations simply by choosing cable companies as their communications providers.

  - ✓ Section 211 **preserved all of the pre-existing standards** in the applicable electronic-surveillance laws.

    - ➢ If agents want to use a **pen register** or **trap-and-trace** device (which record the numbers a telephone dials and from which it receives calls, but do not allow agents to listen to or record the contents of communications) or use a **wiretap** to listen to a cable customer's phone conversations, they still must apply for and receive a **court order**.

    - ➢ If agents want to use a **wiretap**, they must establish **probable cause** that criminal activity is afoot.

Section 212. Emergency disclosure of electronic communications to protect life and limb.

- Summary: Allows computer-service providers to disclose communications in life-threatening emergencies.

- Facts:

  - ✓ Before USA PATRIOT, communications providers **could not disclose records about their customers in emergency situations**. If an Internet service provider learned that a customer was about to commit a terrorist attack, and notified law enforcement, it could be subject to civil lawsuits – even if the disclosure saved lives.

  - ✓ Section 212 allows communications providers **voluntarily to turn over information in emergencies** without fear of civil liability. Now, providers are **permitted – but not required** – to give law enforcement information in emergencies involving a risk of death or serious injury.

    - ➢ This is the equivalent of allowing citizens to tell police that, while walking down a public street, they overheard two people discussing a crime they were about to commit and decided to notify the police.

    - ➢ Section 212 **does not** impose an affirmative obligation to review customer communications in search of such imminent dangers.

  - ✓ Communications providers have used this new authority to disclose vital information to law enforcement in a number of important investigations, including a **bomb threat against a high school**.

    - ➢ An anonymous person posted on an Internet message board a bomb death threat that specifically named a faculty member and several students.

    - ➢ The message board's owner initially resisted giving law enforcement any information about the suspect for fear that he could be sued. Once agents explained section 212, the owner turned over evidence that led to the timely arrest of the individual responsible for the bomb threat.

    - ➢ The message board's owner later revealed that he had been worried for the safety of the students and teachers for several days, and expressed his relief that the USA PATRIOT Act permitted him to help.

  - ✓ Section 212 also played a key role in a case where two unknown individuals, using a U.S.-based email account, threatened to kill **executives at a company in another country** unless they were paid a hefty ransom. The email provider used section 212 to disclose key information about the suspects. The Justice Department then transmitted this information to the authorities in that country, **less than two hours after we were first contacted**. Both suspects later were apprehended overseas.

  - ✓ This provision will sunset on December 31, 2005.

Section 213. Authority for delaying notice of the execution of a warrant.

- Summary: Allows courts, in certain narrow circumstances, to give delayed notice that a search warrant has been executed.

- Myth: "It expands the government's ability to search private property without notice to the owner." [ACLU, Apr. 3, 2003]

- Reality:

  - ✓ Delayed notification warrants are a **long-existing, crime-fighting tool upheld by courts nationwide for decades** in organized crime, drug cases and child pornography.

    - ➢ Section 213 of USA PATRIOT Act simply codified the authority law enforcement already had for decades. Because of differences between jurisdictions, the law was a mix of inconsistent standards that varied widely across the country. This lack of uniformity hindered complex terrorism cases. Section 213 resolved the problem by establishing a **uniform statutory standard**. Section 213 is a vital aspect of our strategy of prevention – detecting and incapacitating terrorists *before* they are able to strike.

  - ✓ **The Supreme Court has held the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant.** The Supreme Court emphasized "that covert entries are constitutional in some circumstances, at least if they are made pursuant to a warrant." In fact, the Court stated that an argument to the contrary was "frivolous." *Dalia v. U.S.*, 441 U.S. 238 (1979). In yet another case, the Court said, "officers need not announce their purpose before conducting an otherwise [duly] authorized search if such an announcement would provoke the escape of the suspect or the destruction of critical evidence." *Katz v. U.S.*, 389 U.S. 347 (1967).

  - ✓ If the **Otter Amendment**, passed in the House July 22, 2003, becomes law, it would have a devastating effect on our ongoing efforts to detect and prevent terrorism, as well as to combat other serious crimes. This amendment could ***tip off*** **terrorists** or criminals to investigations before law enforcement could obtain the needed information to locate their terrorists or criminal associates, identify and disrupt their plans, or initiate their arrests.

    - ➢ Premature notification of a search warrant could result in the **intimidation of witnesses, destruction of evidence, flight from prosecution, physical injury, and even death**.

  - ✓ In all cases, section 213 **requires law enforcement to give notice** that property has been searched or seized. It simply allows agents to **temporarily delay** when the required notification is given.

- ✓ This authority can be used only upon the issuance of a **court order, in extremely narrow circumstances**. Courts can delay notice only when immediate notification may result in **death or physical harm** to an individual, **flight** from prosecution, evidence **tampering**, or witness **intimidation**.

- ✓ Under section 213, courts can delay notice if there is "reasonable cause" to believe that immediate notification may have a specified adverse result. The "reasonable cause" standard is consistent with pre-PATRIOT Act caselaw for delayed notice of warrants. *See, e.g., United States v. Villegas*, 899 F.2d 1324, 1337 (2d Cir. 1990) (government must show "good reason" for delayed notice of warrants).

- ✓ Section 213 is important to law-enforcement investigations of a wide variety of serious crimes, including **domestic and international terrorism**, **drug trafficking**, **organized crime**, and **child pornography**.

  - In *United States v. Odeh*, a recent narco-terrorism case, a court issued a section 213 warrant in connection with the search of an envelope that had been mailed to a target of an investigation. The search confirmed that the target was operating a hawala money exchange that was used to funnel money to the Middle East, including to an individual associated with someone accused of being an operative for Islamic Jihad in Israel. The delayed-notice provision allowed investigators to conduct the search without fear of compromising an ongoing wiretap on the target and several of the confederates. The target was later charged and notified of the search warrant.

  - During an investigation into a nationwide organization that distributes marijuana, cocaine and methamphetamine, the court issued a delayed notice warrant to search the residence in which agents seized in excess of 225 kilograms of drugs. The organization involved relied heavily on the irregular use of cell phones, and usually discontinued the use of cell phones after a seizure of the drugs and drug proceeds, making continued telephone interception difficult. Interceptions after the delayed notice seizure indicated that the suspects thought other drug dealers had stolen their drugs, and none of the telephones intercepted were disposed of, and no one in the organization discontinued their use of telephones. The government was able to prevent these drugs from being sold, without disrupting the larger investigation.

Section 214. Pen register and trap and trace authority under FISA.

- Summary: Allows the United States to obtain a FISA pen register order by certifying that the resulting information would be relevant to an investigation to protect against international terrorism or clandestine intelligence activities.

- Myth: "The amendment significantly eviscerates the constitutional rationale for the relatively lax requirements that apply to foreign intelligence surveillance." [EPIC, Mar. 19, 2003]

- Reality:

  - ✓ Section 214 **streamlined the process** for obtaining pen registers under FISA. It preserved the existing **court-order requirement**. Now, as before, law enforcement cannot install a pen register unless it applies for and receives permission from the FISA court.

  - ✓ Section 214 goes further to protect privacy than the Constitution requires. The Supreme Court has long held that law enforcement is **not constitutionally required to obtain court approval** before installing a pen register.

    - ➢ Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. As such, the Constitution does not require that law enforcement obtain court approval before installing a pen register. This is so because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and "when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company." *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

  - ✓ Section 214 explicitly safeguards **First Amendment rights**. It requires that any "investigation of a United States person is **not** conducted solely upon the basis of activities protected by the First Amendment to the Constitution."

  - ✓ A pen register is a device that can track routing and addressing information about a communication – for example, which numbers a particular telephone dials. Pen registers are not used to collect the content of communications.

  - ✓ Whether the Department has used section 214 is classified. Details about its use were provided to the House Judiciary Committee on May 29, 2003.

  - ✓ This provision will sunset on December 31, 2005.

Section 215. Access to business records and other items under the Foreign Intelligence Surveillance Act.

- Summary: Allows the FISA court, in an investigation to protect against international terrorism or clandestine intelligence activities, to issue an ex parte order requiring the production of any tangible things.

- Myth: "Many [people] are unaware that their library habits could become the target of government surveillance. In a free society, such monitoring is odious and unnecessary. . . The secrecy that surrounds section 215 leads us to a society where the 'thought police' can target us for what we choose to read or what Websites we visit." [ACLU, July 22, 2003]

- Reality:

  - ✓ The library habits of ordinary Americans are of **no interest** to those conducting terrorism investigations. However, historically terrorists and spies *have* used libraries to plan and carry out activities that threaten our national security. **We should not allow libraries to become safe havens for terrorist or clandestine activities.**

  - ✓ Obtaining business records is a long-standing law enforcement tactic. **Ordinary grand juries** for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.

    - ➢ In a recent **domestic terrorism criminal** case, a grand jury served a subpoena on a bookseller to obtain records showing that a suspect had purchased a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.

    - ➢ In the 1997 **Gianni Versace** murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach.

    - ➢ In the 1990 **Zodiac gunman** investigation, a New York grand jury subpoenaed records from a public library in Manhattan. Investigators believed that the gunman was inspired by a Scottish occult poet, and wanted to learn who had checked out his books.

  - ✓ Section 215 authorized the FISA court to issue **similar orders in national-security investigations**. It contains a number of safeguards that protect civil liberties.

    - ➢ Section 215 requires FBI agents to get a **court order**. Agents cannot use this authority unilaterally to compel any entity to turn over its records. FISA orders are *unlike* grand jury subpoenas, which are requested without court supervision.

    - ➢ Section 215 has a **narrow scope**. It can only be used (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect

against international terrorism or clandestine intelligence activities." **It cannot be used to investigate ordinary crimes, or even domestic terrorism.**

- Section 215 preserves **First Amendment rights**. It expressly provides that the FBI cannot conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States."

- Section 215 provides for **congressional oversight**. Every six months, the Attorney General must "fully inform" Congress on how it has been implemented.

- On October 17, 2002, the House Judiciary Committee issued a **press release** indicating it is **satisfied with the Department's use of section 215**: "The Committee's review of classified information related to FISA orders for tangible records, such as library records, has not given rise to any concern that the authority is being misused or abused."

✓ There is much **misinformation – even disinformation** – about the supposed use of section 215 at libraries.

- On November 3, 2002, the *Hartford Courant* alleged that the FBI installed software on computers at the Hartford Public Library that lets agents track a person's use of the Internet and email messages. The article even said that individuals' library use could be surveilled even if they weren't suspected of being a terrorist. In reality, the FBI **obtained a single search warrant** to copy the hard drive of a specific computer that had been used to hack into a business computer system in California for criminal purposes. **No software was installed** on that or any other computer in the library. **The *Hartford Courant* has retracted the story in full.**

✓ Section 215 actually is ***more*** **protective of privacy** than the authorities for ordinary grand jury subpoenas.

- A **court must explicitly authorize** the use of section 215 to obtain business records. By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval.

- Section 215 **expressly protects the First Amendment**, unlike federal grand jury subpoenas.

- Section 215 can only be used, in investigations of U.S. persons, to protect against international terrorism or clandestine intelligence activities. A grand jury can obtain business records in investigations of *any* federal crime.

✓ The requirement that recipients of these orders keep them confidential is **based on "national security letter" statutes**, which have existed for decades. (An NSL is a type of administrative subpoena used in certain national-security investigations.)

- ✓ The details of FISA-related investigations, including requests for business records, are classified. Classified details about the use of section 215 were provided to the House Permanent Select Committee on Intelligence on July 29, 2002, in response to a request by the House Committee on the Judiciary, and to the Senate Select Committee on Intelligence on January 7, 2003, in response to a request by the Constitution Subcommittee of the Senate Committee on the Judiciary.

- ✓ The new tool improved on FISA's original business-records authority in a number of respects:

  - ➢ It expanded the **types of entities** that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." The new provision contains no such restrictions.

  - ➢ It expanded the **types of items** that can be requested. Under the old authority, the FBI could only seek "records." Now, the FBI can seek "any tangible things (including books, records, papers, documents, and other items)."

- ✓ This provision will sunset on December 31, 2005.

Section 216. Modification of authorities relating to use of pen registers and trap and trace devices.

- Summary: Amends the pen register/trap and trace statute (1) to clarify that it applies to Internet communications, and (2) to allow for a single order that is valid across the country.

- Myth: "Section 216 would worsen the problem by giving the FBI access to communications of non-targets and to portions of the target's communications to which it is not entitled under the court order it obtained. The 'trust us, we're the government' solution the FBI proposes is entirely unacceptable and inconsistent with the Fourth Amendment." [ACLU, Oct. 23, 2001]

- Reality:

  - ✓ For years, law enforcement has used pen registers to track which numbers a particular telephone dials. *See* 18 U.S.C. § 3123. Before the USA PATRIOT Act, it was not clear that they could be used to gather the same routing and addressing information about Internet communications.

  - ✓ Section 216 **updated the law to the technology**. It ensures that law enforcement will be able to collect non-content information about terrorists' communications regardless of the media they use.

  - ✓ Section 216 also allows courts to issue pen-register orders that are **valid across the country**. As a result, law enforcement no longer needs to waste precious time by applying for new orders each time an investigation leads to another jurisdiction.

  - ✓ Section 216 **preserved all of the law's pre-existing standards**. As before, law enforcement must get **court approval** before installing a pen register. And as before, law enforcement must show that the information sought is **relevant** to an ongoing investigation.

  - ✓ In fact, section 216 **enhanced the privacy protections** in the pen-register statute. It made explicit that anyone using a pen register has an affirmative obligation to **avoid the collection of content**.

    - ➢ The Department is committed to complying with the Act's mandate that pen registers not be used to capture content. On May 24, 2002, the Deputy Attorney General issued a memorandum instructing field offices to: (1) minimize any possible collection of content; (2) refrain from using any content that may be acquired inadvertently; and (3) coordinate with Department headquarters about what constitutes content.

  - ✓ Department field investigators and prosecutors have used section 216 in a number of terrorism and other important criminal cases.

- Section 216 was used in the investigation of the murder of *Wall Street Journal* **reporter Danny Pearl**, to obtain information that proved critical to identifying some of the perpetrators.

- Section 216 was used in a case where two unknown individuals, using a U.S.-based email account, threatened to kill **executives at a company in another country** unless they were paid a hefty ransom. The use of a pen register enabled Department investigators to provide the foreign authorities with critical information about the suspects' identities – which led to their prompt apprehension overseas.

- Investigators also have used section 216 to collect routing information about the Internet communications of (1) terrorist conspirators; (2) at least one major drug distributor; (3) thieves who obtained victims' bank-account information and stole the money; (4) a four-time murderer; and (5) a fugitive who fled on the eve of trial using a fake passport.

✓ A pen register is a device that can track routing and addressing information about a communication – for example, which numbers a particular telephone dials. Pen registers are not used to collect the content of communications.

✓ Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. As such, the Constitution does not require that law enforcement obtain court approval before installing a pen register. This is so because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and "when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company." *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

✓ The law provides for robust oversight of law enforcement's use of pen registers. The pen register statute has always required that a report be made to Congress every year as to its use. In addition, the USA PATRIOT Act added a requirement that law enforcement report to the supervising court anytime it uses its own pen register to collect Internet information.

Section 217. Interception of computer trespasser communications.

- Summary: Allows victims of computer-hacking crimes to request law-enforcement assistance in monitoring trespassers on their computers.

- Myth: "The new law places the determination solely in the hands of law enforcement and the system owner or operator. . . . [T]he amendment has little, if anything, to do with legitimate investigations of terrorism." [EPIC, Mar. 19, 2003]

- Reality:

  - ✓ The law has always recognized the right of landowners to ask law enforcement to help expel people who illegally trespass on their property.

  - ✓ Section 217 **made the law technology-neutral**, placing cyber-intruders on the same footing as physical intruders. Now, hacking victims can seek law-enforcement assistance to combat hackers, just as burglary victims have been able to invite officers into their homes to catch burglars.

    - ➢ Prior to the enactment of the USA PATRIOT Act, the law prohibited computer service providers from sharing with law enforcement that hackers had broken into their systems.

  - ✓ Computer operators are **not required to involve law enforcement** if they detect trespassers on their systems. Section 217 simply gives them the option of doing so.

  - ✓ Section 217 preserves the **privacy** of law-abiding computer users. Officers cannot agree to help a computer owner unless (1) they are engaged in a **lawful investigation**; (2) there is reason to believe that the communications will be **relevant to that investigation**; and (3) their activities will not acquire the **communications of non-hackers**.

  - ✓ This provision has played a key role in a number of terrorism investigations, national-security cases, and investigations of other serious crimes.

  - ✓ Section 217 is extremely helpful when computer hackers launch massive **"denial of service" attacks** – which are designed to shut down individual web sites, computer networks, or even the entire Internet.

  - ✓ The definition of "computer trespasser" does not include an individual who has a contractual relationship with the service provider. Thus, for example, America Online could not ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers.

  - ✓ This provision will sunset on December 31, 2005.

Section 218. Foreign intelligence information.

- Summary: Encourages an integrated antiterrorism campaign by allowing the use of FISA whenever "a significant purpose" of the investigation is foreign intelligence.

- Myth: "It permits the FBI to conduct a secret search or to secretly record telephone conversations for the purpose of investigating crime even though the FBI does not have probable cause of crime. The section authorizes unconstitutional activity – searches and wiretaps in non-emergency circumstances – for criminal activity with no showing of probable cause of crime." [ACLU, Oct. 23, 2001]

- Reality:

  - ✓ Before the USA PATRIOT Act, **a perceived metaphorical "wall"** often inhibited vital information sharing and coordination. Intelligence investigators were concerned about sharing information with, and seeking advice from, law enforcement investigators and prosecutors. There was a fear that such sharing and consultation could mean that they would not be able to obtain or continue FISA coverage.

    - ➢ Previously, courts had ruled that FISA could be used only when foreign intelligence was the "primary purpose" of an investigation.

  - ✓ Section 218 expressly permitted the **full coordination** between intelligence and law enforcement that is vital to protecting the nation's security. Now, FISA can be used whenever foreign intelligence is a "significant purpose" of a national security investigation. Moreover, section 504 of the USA PATRIOT Act specifically permits intelligence investigators to consult with federal law enforcement officers to coordinate efforts to investigate or protect against threats from foreign powers and their agents.

  - ✓ Generally, a surveillance or search under FISA can be ordered only if the court finds that there is probable cause to believe that the target is a foreign power or an agent of a foreign power.

  - ✓ This provision already is producing important dividends in the war on terror. The Department recently obtained the **indictment of Sami al-Arian**, an alleged member of a Palestinian Islamic Jihad (PIJ) cell in Tampa, Florida.

    - ➢ PIJ is alleged to be one of the world's most violent terrorist outfits. It is responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom.

    - ➢ Section 218 enabled criminal investigators finally to obtain and consider the full range of evidence of the PIJ operations in which al-Arian allegedly participated.

  - ✓ The Department has issued several new **directives that have fostered cooperation** among national-security and law-enforcement personnel.

- The Attorney General instructed all U.S. Attorneys to **review intelligence files** to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. More than 5,000 files have been reviewed as part of this process. Information from this review has been used to open many criminal investigations.

- The Attorney General directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations, and to ensure that information about terrorist threats is shared with other agencies and that criminal charges are considered.

✓ In November of last year, the Foreign Intelligence Surveillance Court of Review **upheld in full** section 218, as well the Department's procedures to implement it.

- The court expressly held "that FISA as amended **is constitutional** because the surveillances it authorizes **are reasonable**." *In re* Sealed Case, 310 F.3d 717, 746 (FISCR 2002).

✓ The old "primary purpose" standard was derived from a number of court decisions, including *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980). That standard was formally established in written Department guidelines in July 1995. While information could be "thrown over the wall" from intelligence officials to prosecutors, the decision to do so always rested with national-security personnel – even though law-enforcement agents are in a better position to determine what evidence is pertinent to their criminal case. The old legal rules discouraged coordination, and created what the Foreign Intelligence Surveillance Court of Review calls "perverse organizational incentives." *In re Sealed Case*, 310 F.3d at 743.

✓ On March 6, 2002, the Department issued guidelines that expressly authorized – and indeed required – coordination between intelligence and law enforcement. These revised procedures were approved in full by the Foreign Intelligence Surveillance Court of Review on November 18, 2002. In December 2002, the Department issue field guidance with respect to the March 2002 procedures and the Court of Review's decision.

✓ In addition to upholding the Department's revised procedures, the Court of Review also noted that the old "wall" standards were not required even *prior to* the USA PATRIOT Act. *See In re Sealed Case*, 310 F.3d at 723-27, 735.

✓ This provision will sunset on December 31, 2005.

Section 219. Single-jurisdiction search warrants for terrorism.

- Summary: Allows courts to issue search warrants that are valid nationwide in terrorism investigations.

- Facts:

  - ✓ Under prior law, a court could only issue a search warrant authorizing searches within its own district. That created **unnecessary delays and burdens** when investigating terrorist networks, which often span a number of judicial districts.

  - ✓ Section 219 **eliminated those time-consuming loopholes**. Now, a court in a district where terrorism-related activities have occurred, upon a showing of probable cause, may issue search warrants that are valid within or outside the district.

  - ✓ Section 219 **preserved all of the pre-existing standards** governing the availability of search warrants. Law enforcement still is required to demonstrate, and courts still must find, **probable cause** that criminal activity is afoot.

  - ✓ Section 219 has **made available resources** that otherwise would have been devoted to administrative tasks, thereby maximizing the law enforcement personnel available to investigate terrorists.

  - ✓ This new tool has been used in a number of important terrorism cases. For example, section 219 enabled prosecutors in Virginia to obtain a single search warrant to simultaneously search multiple offices of affiliated charities in two different states. Such coordination is extremely important in cases where one entity may be able to warn another of an impending search.

Section 220. Nationwide service of search warrants for electronic evidence.

- Summary: Allows courts with jurisdiction over the offense to issue search warrants for communications stored by providers anywhere in the country.

- Facts:

  - ✓ Under previous law, some courts declined to issue search warrants for email stored on servers in other districts. Requiring investigators to obtain warrants in distant jurisdictions has **delayed many time-sensitive investigations**. It also placed an **enormous administrative burden** on districts in which major Internet service providers are located (such as E.D. Va. and N.D. Cal.).

  - ✓ Section 220 allows courts to issue search warrants for electronic evidence outside the district where they are located. Now, courts can compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located.

  - ✓ Section 220 has **made available resources** that otherwise would have been devoted to administrative tasks, thereby maximizing the law enforcement personnel available to investigate terrorists.

  - ✓ This new tool has been used in a number of important terrorism cases. For example, one section 220 search warrant was used in a case in one state regarding an individual who had set up a **website promoting jihad** for an organization in another state. The judge where the case was being brought, who was most familiar with the case, was able to sign the search warrant.

    - ➢ The enhanced ability to obtain this information quickly also has proved invaluable in several sensitive non-terrorism investigations, including: (1) the **tracking of a fugitive**; and (2) a hacker who **stole a company's trade secrets** and then extorted money from the company.

  - ✓ This provision can only be used by **courts with jurisdiction** over the investigation.

  - ✓ This provision will sunset on December 31, 2005.

Section 223. Civil liability for certain unauthorized disclosures.

- Summary: Creates a cause of action and authorizes money damages against the United States if officers disclose sensitive information without authorization.

- Facts:

  - ✓ There have been **no** administrative **disciplinary proceedings or civil actions** initiated under section 223 of the Act for unauthorized disclosures of intercepts.

  - ✓ This provision will sunset on December 31, 2005.

Section 319. Forfeiture of funds in United States interbank accounts.

- Summary: Permits the forfeiture of funds held in United States interbank accounts.

- Facts:

  - ✓ Section 319 allows the government to seize funds subject to forfeiture, which are located in a foreign bank account, by authorizing the seizure of the foreign bank's funds that are held in a correspondent U.S. account.

    - ➢ This is true regardless of whether or not the money in the correspondent account is directly traceable to the money held in the foreign bank account.

  - ✓ The Department has used section 319 in several significant cases.

    - ➢ On January 18, 2001, a federal grand jury indicted James Gibson for various offenses, including conspiracy to commit money laundering, and mail and wire fraud. Gibson, a lawyer, allegedly defrauded his clients, numerous personal injury victims, of millions of dollars by fraudulently structuring settlements. Gibson fled to Belize, depositing some of the proceeds from the scheme in two Belizean banks. The Department's efforts to recover the proceeds initially proved unsuccessful. But following the passage of the USA PATRIOT Act, section 319 was used to serve a seizure warrant on the Belizean bank's interbank account in the United States. The remaining funds were recovered.

    - ➢ In December 2001, the Department also used section 319 to recover almost $1.7 million in funds. This money will be used to compensate the victims of the defendant's fraudulent scheme.

Section 373. Illegal money transmitting businesses.

- Summary: Makes it unlawful to run an unlicensed foreign money transmittal business, and eliminates prior requirement that the defendant have known about the state licensing requirement.

- Facts:

  - ✓ Section 373 has enhanced the government's ability to crack down on unlicensed foreign money-transmittal businesses – which terrorists and their supporters often use to **raise funds for terrorist operations**.

  - ✓ The Department has used section 373 in a number of important terrorism and national-security cases.

    - ➢ On April 30, 2002, a federal jury in Boston convicted Mohamed Hussein for running a foreign money transmittal business (**Barakaat North America, Inc.**) without a license in violation of section 373. The al-Barakaat network was affiliated with and received funding from al Qaeda. In 2000 and 2001, after the Hussein brothers ignored Massachusetts's warning that their business needed to be licensed, nearly $3 million was wired from his Boston bank account to the United Arab Emirates. On July 22, 2002, Mohammed Hussein was sentenced to one and a half years in prison, to be followed by two years of supervised release.

    - ➢ Fourteen out of 15 defendants have pled guilty to charges stemming from an illegal money transmitting business based in the Eastern District of New York, involving **funds sent to Yemen, including over $1 million sent just in March 2002**. The final defendant is a fugitive. The lead defendant, who ran the money-transmitting operation, was sentenced to serve 63 months in federal prison. Consensually monitored telephone calls made during the investigation show that this case has had a major deterrent effect on other hawala operators in the Brooklyn area.

    - ➢ On December 17, 2002, three defendants were indicted in connection with an illegal money transmitting business based in the Northern District of New York, which allegedly sent **$486,000 to Yemen**.

    - ➢ Two individuals have been charged with operating an unlicensed money transmitting business in Kentucky. On November 1, 2002, one of the defendants was convicted of **transferring over $594,000 out of the United States**.

Section 412. Mandatory detention of suspected terrorists; habeas corpus; judicial review.

- Summary: Requires the detention of aliens who are certified as threats to the national security, pending their removal from the United States.

- Myth: "Suspects convicted of no crime may be detained indefinitely in 6 month increments without meaningful judicial review." [ACLU, Feb. 11, 2003]

- Reality:

  - ✓ Section 412 allows the government, with extensive judicial supervision, temporarily to detain terrorist aliens until they are removed from the country. It is the equivalent of **denying bail to a criminal defendant**. Section 412 ensures that terrorists are not released to live among the people they seek to harm.

  - ✓ Law-abiding Americans have nothing to fear from section 412. It applies only to **aliens who engage in terrorism** or otherwise pose a severe threat to the national security. And detention lasts only as long as it takes to remove an alien from the U.S.

  - ✓ An extremely **narrow class of aliens** can be detained under section 412. There must be "reasonable grounds to believe" that the alien: (1) entered the United States to violate **espionage or sabotage** laws; (2) entered to **oppose the government by force**; (3) engaged in **terrorist activity**; or (4) endangers the United States' **national security**.

  - ✓ Section 412 expressly grants aliens the right to **challenge their detention in court**. Aliens may file a habeas petition in any federal district court that has jurisdiction.

  - ✓ The Supreme Court has expressly recognized that detaining aliens may be appropriate in terrorism and other national-security cases: "special arguments might be made for forms of preventive detention and for heightened deference to the judgments of the political branches with respect to matters of national security." *Zadvydas v. Davis*, 533 U.S. 678, 696 (2001).

  - ✓ Once the Attorney General has taken a certified alien into custody, he has seven days to initiate removal proceedings or file criminal charges. If the Attorney General does neither, he is required to release the alien. If an alien has been detained "solely" under section 412, and his removal is unlikely in the foreseeable future, the Attorney General "may" continue to detain him for additional periods of up to six months. Additional detention periods are authorized only if releasing the alien "will" threaten national security or cause harm to "the community or any person."

  - ✓ To date, the Attorney General has not used section 412. Numerous aliens who could have been considered have been detained since the enactment of the USA PATRIOT Act. But it has not proven necessary to use section 412 in these particular cases because traditional administrative bond proceedings have been sufficient to detain these individuals without bond. The Department believes that this authority should be retained for use in appropriate situations.

Section 507. Disclosure of educational records.

- Summary: Allows the Department to seek a court order to obtain educational records that are relevant to an investigation of a grave felony or an act of terrorism.

- Myth: "This means that the Attorney General may obtain the private educational records of a student involved in the Vieques protests by asserting that the records are relevant to a domestic terrorism investigation." [ACLU, Dec. 6, 2002]

- Reality:

  - ✓ Section 507 has an **extremely narrow scope**. Records are available only in investigations of the severest terrorist crimes, such as biological-weapons offenses, chemical-weapons offenses, bombing government property, and destroying airliners.

  - ✓ In order to obtain records under section 507, law enforcement is required to apply for and receive a **court order**. Law enforcement cannot unilaterally compel educational institutions to turn over any information.

  - ✓ Section 507 can only be used if law enforcement certifies to the court that there are "**specific and articulable facts**" giving reason to believe that the records sought contain information relevant to the terrorism crimes being investigated.

  - ✓ Only **high-ranking Department officials** – all of whom are Senate-confirmed – are entitled to ask a court to order the disclosure of records. This ensures accountability.

  - ✓ Section 507 requires the Attorney General to issue guidelines to protect **confidentiality**.

Section 508. Disclosure of information from NCES surveys.

- Summary: Allows the Department to seek a court order to obtain records from the National Center for Educational Statistics that are relevant to an investigation of a grave felony or an act of terrorism.

- Facts:

  - ✓ Section 508 has an **extremely narrow scope**. Records are available only in investigations of the severest terrorist crimes, such as biological-weapons offenses, chemical-weapons offenses, bombing government property, and destroying airliners.

  - ✓ In order to obtain records under section 508, law enforcement is required to apply for and receive a **court order**. Law enforcement cannot unilaterally compel educational institutions to turn over any information.

  - ✓ Section 508 can only be used if law enforcement certifies to the court that there are "**specific and articulable facts**" giving reason to believe that the records sought contain information relevant to the terrorism crimes being investigated.

  - ✓ Only **high-ranking Department officials** – all of whom are Senate-confirmed – are entitled to ask a court to order the disclosure of records. This ensures accountability.

  - ✓ Section 508 requires the Attorney General to issue guidelines to protect **confidentiality**.

Section 801. Terrorist attacks and other acts of violence against mass transportation systems.

- Summary: Makes it a federal offense to engage in terrorist attacks and other acts of violence against mass transportation systems.

- Facts:

  - ✓ The attacks of September 11 confirmed that terrorists are committed to attacking mass transit systems such as airliners. Section 801 created a new offense prohibiting violent offenses against mass transportation systems, vehicles, facilities, or passengers.

  - ✓ The Department recently used section 801 in a case where a **female passenger on a cruise ship** sent threatening notes to the ship's crew. On May 15, 2003, Kelley Marie Ferguson pleaded guilty to making the threats while on board the *Legend of the Seas*, en route to Hawaii.

  - ✓ The Department also attempted to use section 801 in the case of **"shoebomber" Richard Reid**, who now stands convicted of attempting to ignite a bomb hidden in his shoes during an international flight. Reid was sentenced to **life imprisonment**.

    - ➢ A federal judge dismissed the section 801 charge, concluding that an airliner is not a "vehicle" within the meaning of the statute.

    - ➢ Congress fixed this loophole in section 609 of the "Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act of 2003," or "PROTECT Act."

  - ✓ Section 801 prohibits disabling or wrecking a mass transportation vehicle; placing a biological agent or destructive substance or device in a mass transportation vehicle with intent to endanger safety or with reckless disregard for human life; setting fire to or placing a biological agent or destructive substance or device in a mass transportation facility knowing or having reason to know that the activity is likely to disable or wreck a mass transportation vehicle; disabling mass transportation signaling systems; interfering with personnel with intent to endanger safety or with reckless disregard for human life; use of a dangerous weapon with intent to cause death or serious bodily injury to a person on the property of a mass transportation provider; conveying false information about any such offense; and attempt and conspiracy.

  - ✓ The provision carries a maximum sentence of 20 years imprisonment, or life imprisonment if the crime results in death.

Section 802. Definition of domestic terrorism.

- Summary: Adds to 18 U.S.C. § 2331 a new definition of "domestic terrorism," similar to the existing definition of "international terrorism."

- Myth: "Expands terrorism laws to include 'domestic terrorism' which could subject political organizations to surveillance, wiretapping, harassment, and criminal action for political advocacy." [ACLU, Feb. 11, 2003]; The Patriot Act includes "provision that might allow the actions of peaceful groups that dissent from government policy, such as Greenpeace, to be treated as 'domestic terrorism.'" [ACLU fundraising letter, cited by Stuart Taylor, "Backlash Grows against Patriot Act- But Critics Miss the Mark," *Fulton County Daily Report*, Aug. 5, 2003]

- Reality:

  - ✓ Section 802's definition of "domestic terrorism" is **extremely narrow** – indeed, it is much narrower than the pre-existing definition of "international terrorism."

  - ✓ Individuals and groups would be eligible for surveillance under this definition only if they engage in **criminal wrongdoing that could result in death**. That is so because the definition of "domestic terrorism" is limited to conduct that (1) violates federal or state criminal law and (2) is dangerous to human life.

    - ➢ In addition, law enforcement would have to show that the conduct appears to have been committed with a specified terrorism related intent, and that the conduct occurred primarily in the U.S.

    - ➢ By contrast, an individual would fall within the definition of "international terrorism" whenever he or she commits a crime that involves "**violent"** conduct.

Section 805. Material support for terrorism.

- Summary: Strengthens the existing ban on providing material support to terrorists and terrorist organizations.

- Facts:

  - ✓ Before the PATRIOT Act, it was not certain that the ban on "material support or resources" encompassed expert advice and assistance – for example, advice provided by a civil engineer on destroying a building, or advice by a biochemist on making a biological agent more lethal.

  - ✓ Section 805 enhanced the material-support statute in several crucial respects, including by making it expressly apply to those who provide **expert advice or assistance** to terrorists.

  - ✓ Other changes that section 805 made to the material-support statute include: (1) making it apply to acts outside the United States; (2) expanding the list of terrorism crimes for which it is illegal to provide material support; and (3) clarifying that material support includes all types of monetary instruments. Section 810 increased the maximum penalties for providing material support from 10 years to 15 years.

Section 806. Assets of terrorist organizations.

- Summary: Amends federal forfeiture law to authorize civil forfeiture of assets owned by persons engaged in terrorism.

- Myth: "Section 806 of the Act could result in the civil seizure of their assets without a prior hearing, and without them ever being convicted of a crime. It is by far the most significant change of which political organizations need to be aware." [ACLU, Dec. 6, 2002]

- Reality:

  - ✓ Forfeiture under section 806 is authorized only in **narrow circumstances**. The subject must be engaged in conduct that (1) violates **federal or state criminal law**; (2) involves **violence or the risk of death**; and (3) is committed with a **terrorist intent**.

  - ✓ Prior law **did not specifically authorize the confiscation of terrorist assets**. Instead, forfeiture was authorized only in narrow circumstances for the "proceeds" of murder, arson, and some terrorism offenses. But most terrorism offenses do not yield proceeds, and available forfeiture laws required detailed tracing that is difficult for accounts coming through the banks of countries used by many terrorists.

  - ✓ Section 806 increases our ability to **strike at terrorists' economic base** by permitting the forfeiture of their property regardless of the source of the property, and regardless of whether the property has actually been used to commit a terrorism offense.

  - ✓ Section 806 is **similar to the forfeiture previously available under RICO**. In parity with the drug forfeiture laws, the section also authorizes the forfeiture of property used or intended to be used to facilitate a terrorist act, regardless of its source.

  - ✓ As of April 1, 2003, the Department **has not yet used section 806**. In most cases, it has not been necessary for the Department to seek forfeiture under this provision, because the suspects' assets already had been frozen by the Treasury Department.

Section 812. Post-release supervision of terrorists.

- Summary: Courts may authorize post-release supervision periods of up to life for persons convicted of terrorism crimes that involved the occurrence or foreseeable risk of death or serious injury

- Facts:

  - ✓ Prior federal law generally capped the maximum period of post-imprisonment supervision for released felons at **3 or 5 years**. The **drug laws** mandate longer supervision periods for persons convicted of certain drug crimes, and specify no upper limit on the duration of supervision, but before the PATRIOT Act there was nothing comparable for terrorism offenses.

  - ✓ Thus, for a released but unreformed terrorist, there was no means of tracking the person or imposing conditions to prevent renewed involvement in terrorist activities beyond a period of a few years.

  - ✓ Section 812 authorized **longer supervision periods**, including potentially lifetime supervision, for persons convicted of certain terrorism crimes. This permits appropriate **tracking and oversight** following release of offenders whose involvement with terrorism may reflect lifelong ideological commitments.

  - ✓ In order to qualify for post-release supervision under section 812, one must have committed a specified terrorism-related crime, and the offense must have resulted in, or created a foreseeable risk of, **death or serious injury**.